UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MICHAEL LOVETRO on behalf of himself and all others similarly situated, Plaintiff, v. AT&T, INC., Defendant.	**CLASS ACTION** Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Michael Lovetro, through his attorneys, brings this Class Action Complaint against the Defendant, AT&T, Inc. ("AT&T" or "Defendant"), alleging as follows:

INTRODUCTION

1. On or around March 30, 2024, AT&T, a giant in the telecommunications industry, announced it had lost control over its computer network and the highly sensitive private information stored on the computer network in a data breach by cybercriminals ("Data Breach").

2. Due to its deliberately obfuscating language, it is unclear when the unauthorized party first gained access to Defendant's network and how long cybercriminals had unfettered excess to Plaintiff's and the Class's sensitive and private information. Following the Breach, Defendant has been conducting an ongoing internal investigation which has revealed that cybercriminals gained unauthorized access to former and current customers' personally identifiable information ("PII"), including but not limited to their full names, email addresses,

mailing addresses, date of birth, phone numbers, AT&T account numbers and passcodes, and Social Security numbers ("personally identifiable information" or "PII").

3. On or around March 31, 2024, Defendant began notifying victims about the breach. During this time, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. AT&T failed to reasonably secure, monitor, and maintain the PII provided to it by its former and current customers. Upon information and belief, the Data Breach resulted in the likely unauthorized access, download, exfiltration, and misuse of the PII by the cyber criminals who targeted that information through their wrongdoing.

5. As a result of the Data Breach, Plaintiff and approximately 73 million Class Members (including 7.6 million current customers and 65.4 million former customers)[1], suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is

[1] *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, The New York Times, https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html (last accessed April 2, 2024).

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its victims how many people were impacted, how the breach happened, or why AT&T delayed notifying its victims that hackers had gained access to highly sensitive PII.

7. Defendant's failure to timely detect and report the Data Breach made its customers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect customers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its former and current customers.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and the Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is an AT&T customer and a Data Breach victim.

12. Accordingly, Plaintiff, on behalf of himself and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Michael Lovetro, is a natural person, resident, and citizen of Georgia, where he intends to remain. Mr. Lovetro is a Data Breach victim.

14. Defendant AT&T, Inc. is a corporation organized under the state laws of Delaware with its headquarters and principal place of business located at 208 S. Akard St. Dallas, TX 75202. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201. Defendant is a citizen of Texas.

JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because its principal place of business is in the Dallas Division of the Northern District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District. The Defendant is a citizen of Texas.

17. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

BACKGROUND FACTS

AT&T

18. Defendant is one of the largest wireless carriers and internet providers in the country.

19. On information and belief, AT&T accumulates highly sensitive PII Information of its customers, including names, dates of birth, phone numbers, Social Security numbers, and other sensitive information.

20. Upon information and belief, in the course of collecting PII from customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

21. Defendant provides on its website that: "We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information."[2]

22. AT&T understood the need to protect its customers' data and prioritize its data security. However, despite recognizing its duty to do so, on information and belief, AT&T has not in fact implemented reasonably cybersecurity safeguards or policies to protect its customers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, AT&T leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to former and current customers' PII.

AT&T Fails to Safeguard Customer PII

23. Plaintiff is a customer of AT&T.

[2] AT&T Privacy Notice, AT&T, https://about.att.com/privacy/privacy-notice.html, (last accessed April 2, 2024).

24. As a condition of receiving services with AT&T, Plaintiff provided Defendant with his PII. Defendant used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain services.

25. In collecting and maintaining customers' PII, AT&T implicitly agrees it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

26. In or about March 2024, the details of 73 million former and current AT&T Customer accounts, including full names, email addresses, mailing addresses, phone numbers, dates of birth, social security numbers, AT&T account number and passcode were leaked online.[3] "Details of the leaked data first appeared online in August 2021, when a known threat actor, ShinyHunters, offered up the records for sale on a hacking forum, with a 'buy it now' price of one million dollars."[4] In March 2024, "that same data appears to have been made available for free by another threat actor, MajorNelson."[5]

27. According to the Breach Notice, AT&T claims to discovered that customer information "have been compromised." Ex. A. Following its ongoing internal investigation, AT&T admitted that the information involved in the breach varied by customer but "may have included full name, email address, mailing address, phone number, [S]ocial [S]ecurity number, date of birth, AT&T account number and passcode." *Id*. In other words, Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems allowed those responsible for the cyberattack to obtain files containing millions of AT&T former and current customers' PII.

---

[3] *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, The New York Times, https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html (last accessed April 2, 2024).
[4] *Id.*
[5] *Id.*

28. Further, Defendant has admitted that customers' information has been released on the dark web, stating that "AT&T data-specific fields were contained in a data set released on the dark web."[6]

29. Despite its duties and alleged commitments to safeguard PII, AT&T does not follow industry standard practices in securing former and current customers' PII, as evidenced by the Data Breach.

30. In response to the Data Breach, Defendant contends that it has or will be "working with cybersecurity experts to analyze the situation." Ex. A. Although Defendants fail to provide information on any steps they are taking to remediate the situation. Regardless, any remedial steps should have been in place before the Data Breach.

31. Through its online Breach Notice, AT&T recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims "remain vigilant by monitoring account activity and credit reports" advising that victims should place "set up free fraud alerts from nationwide credit bureaus." Ex. A.

32. On information and belief, AT&T has offered complimentary credit monitoring services to customers whose personal information was compromised, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

33. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other

[6] *Keeping your account secure,* AT&T, https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last accessed April 2, 2024).

sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

34. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine this with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

35. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

36. On information and belief, AT&T failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its former and current customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Plaintiff's Experience

37. Plaintiff is an ATT&T customer and a Data Breach victim.

38. As a condition of utilizing Defendant's services, Mr. Lovetro provided his PII to AT&T and trusted that the company would use reasonable measures to protect it according to AT&T's internal policies and state law.

39. Mr. Lovetro reasonably believed that a portion of the funds he paid to AT&T for its services would be used for adequate cybersecurity protection for his PII.

40. Mr. Lovetro received notice of the Breach on or about March 30, 2024 when Defendant publicly confirmed the breach, stating: " AT&T* has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago." *AT&T Addresses Recent Data Set Released on*

the Dark Web, https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed April 2, 2024).

41. Due to AT&T's obfuscating language, it was unclear to Plaintiff precisely which of his PII was exposed, how the Data Breach occurred, and how long cybercriminals had unfettered access to his PII.

42. AT&T deprived Plaintiff of the earliest opportunity to guard his PII against the Data Breach's effects by failing to immediately and promptly notify him about it.

43. As a result of the Data Breach Plaintiff has several hours of his time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his information to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

44. Mr. Lovetro fears for his personal financial security and uncertainty over what PII exposed in the Data Breach. Mr. Lovetro has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

45. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

46. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

47. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

48. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

49. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

50. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

51. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, date of birth, or Social Security number, without permission, to commit fraud or other crimes.

52. The types of PII compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The customers' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

53. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

54. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and

refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

55. As a result of AT&T's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

56. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

57. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

58. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

59. One such example of criminals using PII for profit is the development of "Fullz" packages.

60. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

61. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

62. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

63. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by its complete failure to prevent malware in its systems, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and the Class to unscrupulous operators, con-artists, and criminals.

64. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest

ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

65. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

66. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[7]

67. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Ty Inc. knew or should have known that its electronic records would be targeted by cybercriminals.

68. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

69. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

70. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including

[7] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed April 2, 2024).

ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

71. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[8]

72. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[9]

73. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[10]

74. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities

[8] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed April 2, 2024).
[9] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed April 2, 2024).
[10] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed April 2, 2024).

such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

75. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of millions of its current and former customers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

76. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

77. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its customers' PII to protect against their publication and misuse in the event of a cyberattack.

Defendant failed to adhere to FTC guidelines.

78. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

79. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

80. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

81. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to former and current customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

84. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

85. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

86. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

88. Plaintiff sues on behalf of himself and the proposed Class ("Class"), defined as follows:

> **All individuals in the United States whose PII was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.**

89. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

90. Plaintiff reserves the right to amend the class definition.

91. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

92. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of millions of members, far too many to join in a single action;

93. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

94. **Typicality.** Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

95. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with Class members' interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

96. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant was negligent in maintaining, protecting, and securing PII;

d. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendant's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class's injuries;

h. What the proper damages measure is; and

i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

97. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

98. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

99. Plaintiff and members of the Class entrusted their PII to AT&T. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized

parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

100. AT&T was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's PII on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

101. Defendant knew that the PII of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

102. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's PII was provided to AT&T with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

103. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain

adequate security measures to safeguard that information and allowing unauthorized access to Plaintiff's and the Class's PII.

104. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

105. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII.

106. As a result of Defendant's failure, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

107. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

108. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

110. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

111. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

112. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

113. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

114. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

115. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and the Class would not have been injured.

116. The injury and harm suffered by Plaintiff and the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

117. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Intrusion upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiff and the Class)

118. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

119. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts§ 652B (1977).

120. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

121. Defendant owed a duty to its current and former customers, including Plaintiff and the Class, to keep this information confidential.

122. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class members' PII is highly offensive to a reasonable person.

123. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

124. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

125. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

126. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

127. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

128. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

129. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

130. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

131. In addition to injunctive relief, Plaintiff, on behalf of themselves and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

133. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving services from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for services with Defendant.

134. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for its telecommunication services.

135. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

136. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiff's and Class Member's PII.

137. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

138. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

139. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

140. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

141. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

142. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

143. In these and other ways, Defendant violated its duty of good faith and fair dealing.

144. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

145. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the Classes)

146. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

147. This claim is pleaded in the alternative to the breach of implied contract claim.

148. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its provision of services and its collection of payment.

149. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII, as this was used to facilitate its provision of services and its collection of payment.

150. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

151. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

152. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

153. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII.

154. Plaintiff and Class members have no adequate remedy at law.

155. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

156. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

157. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff's and Class members' PII; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

158. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

159. Because of the highly sensitive nature of the PII, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

160. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

161. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

162. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VII
Breach of Confidence
(On Behalf of Plaintiff and the Class)

163. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

164. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members were provided to Defendant in exchange for its services.

165. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

166. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

167. Plaintiff and Class Members also provided their respective PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

168. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

169. Due to Defendant's failure to prevent, detect, and/or avoid the data breach from occurring by, inter alia, failing to follow best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

170. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

171. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

172. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

173. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives, including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

174. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VIII
Breach of Express Contract
On Behalf of Plaintiff and the Class

175. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

176. Defendant provides telecommunication services to Plaintiff and Class Members pursuant to the terms of its contracts, which all were a party to, including agreements regarding the handling of their confidential PII in accordance with AT&T's policies, practices, and applicable law. Plaintiff is not in possession of these contracts but upon information and belief these contracts are in the possession of AT&T.

177. As consideration, Plaintiff and Class Members paid money to Defendant for its telecommunication services. Accordingly, Plaintiff and Class Members paid Defendant to securely maintain and store their PII.

178. Defendant knew that if it were to breach these contracts, Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

179. Defendant violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' PII and by disclosing it for purposes not required or permitted under the contracts.

180. As reasonably foreseeable result of the breach, Plaintiff and Class Members have been damaged by AT&T's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

PRAYER FOR RELIEF

181. Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: April 2, 2024

Respectfully submitted,

SHAMIS & GENTILE P.A.

/s/ Andrew Shamis
Andrew J. Shamis
Texas Bar No. 24124558
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

Attorneys for Plaintiff and the Proposed Class